Appendix H. Information Technology Standards

ORGANIZATION OF INFORMATION TECHNOLOGY STANDARDS

Electronic commerce (EC) standards are categorized as follows:

- Voluntary industry standards. These are standards developed by nationally and internationally recognized standards bodies, voluntary bodies, consortia, and various international treaties and multilateral and bilateral agreement bodies. Figure H-1 shows some of the key voluntary industry standards bodies (along with their associated standards) that are of interest to Federal EC.

Figure H-1. Key Voluntary Industry Standards Bodies

- Federal standards. These are standards adopted or developed by Federal agencies for use in the government. Although only one published Federal EC related standard [Federal Information Processing Standard (FIPS) 161] exists to date, this anticipates additional Federal standards.

- Department-unique standards. These are standards adopted or developed by individual departments or agencies specifically for their use, e.g., Military Standards. Agencies should only develop unique EC standards when Federal and voluntary industry standards cannot meet their requirements. They must closely coordinate such unique standards with existing Federal and voluntary industry standards activities.

VOLUNTARY INDUSTRY STANDARDS

The EC standards program uses Federal representatives accredited through the program to ensure consideration of U.S. government interests in the work of the external EC standards forums. This is the principal means of fostering the adoption and development (including the consideration of unique Federal needs) of EC standards for government use. It is essential to clearly state and support Federal requirements in external standards bodies if government is to successfully adopt voluntary industry EC standards. The government must address a number of different processes to meet its standards' needs.

The EC process promotes the development and use of national and international voluntary industry standards for implementation in Federal information systems, achieving economy of cost and schedule. Voluntary industry EC standards are developed by nationally recognized voluntary industry standards organizations for use by the general public, various industry consortia for use by specific interest groups, and international treaty and bilateral/multilateral organizations. Commercial activities (industrial groups, joint ventures, and industry leaders pursuing market share) heavily support the first two approaches. The last approach involves a mix of Federal departments and agencies. Currently, EC standards activities do not require participation in Treaty Standards Bodies. However, expansion of the EC scope into other functional areas may require such participation in the future.

VOLUNTARY INDUSTRY STANDARDS BODIES

A number of voluntary industry standards organizations develop, approve, and publish EC standards. One such organization is the American National Standards Institute (ANSI), which serves as the clearinghouse for national standards. It acts as the national body for U.S. participation in the International Organization for Standardization (ISO). It also represents the United States in the United Nations charter body of the Electronic

Data Interchange for Administration, Commerce and Transport (UN/EDIFACT).

The ANSI accredits standards development organizations (SDOs) and standards development committees (SDCs) that agree to work under the ANSI procedures. This guarantees standards development in an open forum in which all interested parties can participate. Accreditation also permits publication of the standards developed by these SDOs and SDCs as American National Standards. ANSI Accredited Standards Committee (ASC) X12 was established to develop EC standards. The Department of Commerce recognized ASC X12 as an approved source for national EC standards in FIPS-161. ASC X12 accredits Federal activities as SDOs. These activities also use the ANSI X12 procedures to promote draft standards they develop as American National Standards in accordance with ASC X12.

VOLUNTARY INDUSTRY STANDARDS POLICY

The OMB Circular A-119 encourages all Federal agencies to participate in developing national standards to satisfy their needs. Departments and agencies provide support, principally by submitting comments on standards issues to the Department of Commerce [National Institute of Standards and Technology (NIST)]. It coordinates the views of all Federal agencies to present a single unified government position. Representatives at the development level ensure the recognition of Federal needs and initiate actions to consider incorporating those needs into ASC X12 standards. The government also seeks to influence the direction of standards work at the executive level by providing representation to selected national and international standards policy body organizations and committees. These executive level organizations include those concerned with standards approval, planning, policy, operations, and management issues.

FEDERAL STANDARDS

Federal EC standards fall under two Federal standards programs. Automated data processing (ADP) standards, as defined by the Brooks Act, are the responsibility of NIST, with the Secretary of Commerce as approval authority. These ADP standards are published as Federal Information Processing Standards (FIPS). The second program, telecommunications standards (those areas specifically excluded by the Brooks Act from the ADP standards definition), is the responsibility of the

National Communications System with the General Services Administration (GSA) as approval authority.

FEDERAL STANDARDS POLICY

Paragraph 201-20.303 of the Federal Information Resources Management Regulation (FIRMR), dated 1 October 1990, specifies policy concerning Federal standards use in FIPS resources acquisitions. It requires personnel to review each standard for applicability to the agency requirement and to ensure the inclusion of all applicable Federal standards in a solicitation. The policy also encourages government agencies to use interim Federal standards when acquiring FIPS resources. The policy states that agencies should consider using voluntary national and international standards when Federal standards do not exist. When no voluntary standards exist, the policy permits the development and use of Department-unique standards. NIST coordinates these agency-unique standards. They cannot violate the "Competition in Contracting Act." Agency heads may allow the use of alternative standards for the acquisition and use of computer security items, provided that such standards are more stringent than the applicable Federal standards. They must also contain, at a minimum, the functional provisions of the applicable Federal standard. As a further note, the Secretary of Commerce granted FIPS waiver authority to the heads of executive departments and agencies on November 14, 1988.

NIST-RELATED FEDERAL STANDARDS ACTIVITIES

NIST has established special workshops and special interest groups, such as the North American Open Systems Environment (OSE) Implementers Workshop, to obtain assistance from the Federal agencies and industry on new standards requirements. When ASC X12 or EDIFACT approves new national or international standards, NIST proposes draft FIPS based on those standards if the voluntary standard has reached a sufficient level of technical maturity to warrant Federal adoption. FIPS PUB 161 adopts two families of EC information syntax standards: ASC X12 for domestic information exchanges and EDIFACT for international information exchanges.

New guidance may be issued by NIST to Federal agencies as FIPS PUB 161-2 as the deadline for conversion of new development to UN/EDIFACT approaches, but only after it becomes clear what the least-cost path is. The government uses EDI with many

interchange partners, and as a result of the administration's recent initiative, will soon use EDI with many more. In 1994, most industries are continuing to develop transaction sets in the original X12 syntax. Whether the government should change to UN/EDIFACT in its interchanges with members of a particular industry may depend on what makes business sense for interchange partners in that industry, including the government. Activity in response to the government initiative in 1994 through 1996 will most likely result in more partnerships that use the original syntax than UN/EDIFACT. For a revised policy, maximizing economy and efficiency in the government and minimizing costs imposed on U.S. businesses would seem to remain valid objectives.

STANDARDS PROFILE

Profiles play an essential role in the implementation of EC standards, serving as the vehicle by which requirements become implemented within the acquisition process. Standards profiles identify the appropriate base standards and specify the classes, subsets, parameter values, and other details from within the base standard. Such profiles are needed to achieve interoperability among the different implementations that support a given functional requirement. Standards profiles may range across a number of levels of specificity. They include the base standards—i.e., ANSI X12; national standards—i.e., Government Open Systems Interconnection Profile (GOSIP); and Federal standards—i.e., FIPS; as well as specific procurement specifications. The standards profile concept, based on the ISO concept of functional profiles, is similar to the NATO concept of functional profiles. Base standards, the foundation for all profiles, specify procedures and formats that facilitate the exchange of information between systems. EC calls profiles implementation conventions.

APPLICABLE STANDARDS

Federal Information Resources Management (IRM) and telecommunications standards apply to all aspects of the architecture. NIST's FIPS and GSA's Federal standards must be used when applicable. If no Federal standard exists, national or international standards must be used. Proprietary products may be used only in areas where no Federal, national, or international standard exists. There are specific sets of standards in place for data interchange services, data base management services, communications services and security services, described in the

NIST application portability profile for the open systems environment. All the standards cannot be addressed in the space available here; however, some critical ones for EC are discussed.

For electronic commerce (EC) in the Federal government, all FIPSs and Federal standards are applicable. The applicable national and international standards are as follows:

- American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 Electronic Data Interchange (EDI)
- ANSI ASC X12.56 Interconnect Mailbag Control Structure
- International Telecommunication Union—Telecommunication Standardization
- Sector X.400 (Version 1988)
- International Telecommunication Union—Telecommunication Standardization
- Sector X.435
- International Telecommunication Union—Telecommunication Standardization
- Sector X.500 (1993)
- File transfer, access, and management (FTAM) over open system interconnectivity (OSI)
- File transfer protocol (FTP) or UNIX-to-UNIX Copy Program (UUCP) over TCP/IP
- Simple mail transfer protocol (SMTP).

The government will provide standard implementation conventions (IC) for the ANSI ASC X12 transactions sets listed below:

- 810—Invoice
- 820—Remittance Advice
- 840—Request for Quotation
- 843—Response to Request for Quotation
- 850—Order or Delivery Order
- 997—Functional Acknowledgment.

Additional implementation conventions and transactions will be standardized based on the government requirements and the completed IC and agreements within the ANSI committees.

ASC X12 AND UN/EDIFACT STANDARDS

In 1979 ANSI chartered the ASC X12, electronic data interchange, to develop uniform standards for electronic interchange of business transactions. The X12 committee develops standards to facilitate electronic interchange relating to such business transactions as order placement and processing, shipping and receiving, invoicing, payment, and cash application data associated with the provision of products and services. The X12 transaction sets generally map a traditional paper document such as those mentioned above to an electronic format that can be passed easily over telecommunication networks. Each transaction format includes many segments that contain the data needed for the business function as well as instructive information to ensure that the telecommunication system routes the data to the correct place. Examples of some ANSI ASC X12 transactions are 838, Vendor Registration; 840, Request for Quotation; 843, Response to Request for Quotation; 850, Purchase Order or Delivery Order; 855, Purchase Order Acknowledgment; and 997, Functional Acknowledgment. These X12 transactions are transmitted to the trading partner (TP) by using either the X12.56 mailbag protocol, the X400 E-mail protocol, or the SMTP or Multipurpose Internet Mail Extensions (MIME) protocols.

If the Federal government uses these transaction sets to support its “single face to industry,” small businesses can still interact with the government using business bureaus or the services of other providers, such as VANs, that will transform the document into a format the business can utilize. For example, if the small business has only fax machines, it need the document in that format rather than ASC X12. By the same token, the government will expect it back in ASC X12 format, so trading partners need a service that can provide that. Just because the Federal government uses ASC X12 to standardize the transmission of documents, small businesses will not be excluded. As discussed elsewhere in this document, X12 will enhance their ability to participate in the Federal procurement process.

At some point in 1997, ASC X12 will cease to develop new standards. All new efforts will be devoted to merging the ASC X12 standards into those of UN/EDIFACT. When work begins on the

EDIFACT standards, the Federal government will still need to maintain the ASC X12 standards well into the next century. The two standards must coexist in every system during this transition. In fact, many government agencies will require EDIFACT initially in order to trade with international partners.

TECHNICAL IPS STANDARDS

The messaging applications for the Internet Protocol Suite (IPS) have evolved significantly over the past few years. The Simple Mail Transfer Protocol (SMTP). SMTP provides a common specification for the exchange of E-mail messages between systems and networks. The MIME protocol has been developed for sending multipart and multimedia E-mail messages. MIME supports binary files, audio messages, and digital video. The key requests for comments (RFCs) are as follows:

- RFC 1523, "The text/enriched MIME Content-type," N. Borenstein, September 1993
- RFC 1522, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies," K. Moore, September 1993
- RFC 1521, "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies," N. Borenstein, N. Freed, September 1993
- RFC 1496, "Rules for Downgrading Messages from X.400/88 to X.400/84 When MIME Content-Types are Present in the Messages," H. Alvestrand, J. Romaguera, K. Jordan, August 1993
- RFC 1441, "SMTP Introduction to version 2 of the Internet-standard Network Management Framework," J.D. Case, M.T. Rose, K. McCloghrie, S. Waldbusser, April 1993
- RFC 1437, "Extension of MIME content-types to a new medium," N. Borenstein, M. Linimon, April 1993
- RFC 1428, "Transition of Internet Mail from Just-Send-8 to 8 bit-SMTP/MIME," G.M. Vaudreuil, February 1993
- RFC 1427, "SMTP Service Extension for Message Size Declaration," J. Klensin, N. Freed, K. Moore, February 1993
- RFC 1426, "SMTP Service Extension for 8 bit-MIME Transport," J. Klensin, N. Freed, M.T. Rose, E.A. Stefferud, February 1993

- RFC 1425, "SMTP Service Extension," J. Klensin, N. Freed, M.T. Rose, E.A. Stefferud, D. Crocker, February 1993
- RFC 1344, "Implications of MIME for Internet mail gateways," N. Borenstein, June 1992
- RFC 1341, "MIME (Multipurpose Internet Mail Extensions): Mechanisms for specifying and describing the format of Internet message bodies," N. Borenstein, N. Freed, June 1992
- RFC 1090, "SMTP on X.25," R. Ullmann, February 1989
- RFC 1047, "Duplicate messages and SMTP," C. Partridge, February 1988
- RFC 876, "Survey of SMTP implementations," D. Smallberg, September 1983
- RFC 821, "Simple Mail Transfer Protocol," J.B. Postel, August 1982
- RFC 788, "Simple Mail Transfer Protocol," J.B. Postel, November 1981
- RFC 780, "Mail Transfer Protocol," S. Sluizer, J.B. Postel, May 1981
- RFC 772, "Mail Transfer Protocol," S. Sluizer, J.B. Postel, September 1980.

The following RFCs on directory services have been published:

- RFC 1107, "Plan for Internet Directory Services," K. Sollins
- RFC 1275, "Replication Requirements to provide an Internet Directory using X.500," S. Hardcastle-Kille
- RFC 1308, "Executive Introduction to Directory Services Using the X.500 Protocol," C. Weider, J. Reynolds
- RFC 1309, "Technical Overview of Directory Services Using the X.500 Protocol," C. Weider, J. Reynolds, S. Heker
- RFC 1430, "A Strategic Plan for Deploying an Internet X.500 Directory Service," S. Hardcastle-Kille, E. Huizer, V. Cerf, R. Hobby, S. Kent
- RFC 1491, "A Survey of Advanced Usages of X.500," C. Weider, R. Wright.

PRIVACY ENHANCED MAIL

Privacy enhanced mail (PEM) is a family of (RFCs that are intended to define a method of providing security services for confidentiality, authentication, message integrity assurance, and nonrepudiation of origin. The current RFCs for PEM are as follows:

- RFC 1424, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services," B.S. Kaliski, February 1993
- RFC 1423, "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers," D. Balenson, February 1993
- RFC 1422, "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management," S.T. Kent, February 1993
- RFC 1421, "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures," J. Linn, February 1993.

PEM was designed and specified to handle RFC 822 messages. RFC 1424 defines message encryption and authentication procedures to provide PEM services for electronic mail transfer in the Internet.

RFC 1423 is organized into four primary sections dealing with message encryption algorithms, message integrity check algorithms, symmetric key management algorithms, and asymmetric key management algorithms (including both asymmetric encryption and asymmetric signature algorithms).

RFC 1422 defines a supporting key management architecture and infrastructure, based on public-key certificate techniques, to provide keying information to message originators and recipients. The key management architecture described in this document is compatible with the authentication framework described in CCITT 1988 X.509. RFC 1422 goes beyond X.509 by establishing procedures and conventions for a key management infrastructure for use with PEM and with other protocols, from both the TCP/IP and OSI suites, in the future. There are several motivations for establishing these procedures and conventions (as opposed to relying only on the very general framework outlined in X.509):

- It is important that a certificate management infrastructure for use in the Internet community accommodate a range of clearly articulated certification policies for both users and organizations in a well-architected fashion. Mechanisms must be provided to enable each user to be aware of the policies governing any certificate which the user may encounter. This requires the introduction and standardization of procedures and conventions that are outside the scope of X.509.

- The procedures for authenticating originators and recipient in the course of message submission and delivery should be simple, automated and uniform despite the existence of differing certificate management policies. For example, users should not have to engage in careful examination of a complex set of certification relationships in order to evaluate the credibility of a claimed identity.

- The authentication framework defined by X.509 is designed to operate in the X.500 directory server environment. However X.500 directory servers are not expected to be ubiquitous in the Internet in the near future, so some conventions are adopted to facilitate operation of the key management infrastructure in the near term.

- Public key cryptosystems are central to the authentication technology of X.509 and those which enjoy the most widespread use are patented in the United States. Although this certification management scheme is compatible with the use of different digital signature algorithms, it is anticipated that the RSA cryptosystem will be used as the primary signature algorithm in establishing the Internet certification hierarchy. Special license arrangements have been made to facilitate the use of this algorithm in the U.S. portion of Internet environment.

RFC 1421 prescribes protocol extensions and processing procedures for RFC-822 mail messages, given that suitable cryptographic keys are held by originators and recipients as a necessary precondition. Privacy enhancement services (confidentiality, authentication, message integrity assurance, and nonrepudiation of origin) are offered through the use of end-to-end cryptography between originator and recipient processes at or above the user agent level. No special processing requirements are imposed on the message transfer system at endpoints or at intermediate relay sites. This approach allows privacy enhancement facilities to be incorporated selectively on a site-by-site or user-by-user basis without impact on other Internet

entities. Interoperability among heterogeneous components and mail transport facilities is supported.

The current specification's scope is confined to PEM processing procedures for the RFC-822 textual mail environment, and defines the content-domain indicator value "RFC822" to signify this usage. Follow-on work in integration of PEM capabilities with other messaging environments such as MIME, is anticipated and will be addressed in separate and/or successor documents, at which point additional content-domain indicator values will be defined.

These services are offered through the use of end-to-end cryptography between originator and recipient processes at or above the user agent level. No special processing requirements are imposed on the message transfer system at endpoints or at intermediate relay sites. This approach allows privacy enhancement facilities to be incorporated selectively on a site-by-site or user-by-user basis without impact on other Internet entities. Interoperability among heterogeneous components and mail transport facilities is supported.

The procedures defined in the current PEM documents are intended to be compatible with a wide range of key management approaches, including both symmetric, or single key, and asymmetric, or public key, approaches for encryption of data encrypting keys. RFC 1422 specifies supporting key management mechanisms based on the use of public-key certificates. RFC 1423 specifies algorithms, modes, and associated identifiers relevant to RFC 1422 and RFC 1421. RFC 1424 provides details of paper and electronic formats and procedures for the key management infrastructure being established in support of these services.

The facilities discussed in RFC 1421 provide privacy enhancement services on an end-to-end basis between originator and recipient processes residing at the UA level or above.

If an originator elects to perform PEM processing on an outbound message, all PEM-provided security services are applied to the PEM message's body in its entirety.

Selective application to portions of a PEM message is not supported. Authentication, integrity, and (when asymmetric key management is employed) nonrepudiation of origin services are

applied to all PEM messages; confidentiality services are optionally selectable.

In keeping with the Internet's heterogeneous constituencies and usage modes, the measures defined here are applicable to a broad range of Internet hosts and usage paradigms. In particular, it is worth noting that the mechanisms defined in this RFC are not restricted to a particular host or operating system, but rather allow interoperability among a broad range of systems. All privacy enhancements are implemented at the application layer and are not dependent on any privacy features at lower protocol layers.

The defined mechanisms are compatible with nonenhanced Internet components. Privacy enhancements are implemented in an end-to-end fashion which does not impact mail processing by intermediate relay hosts which do not incorporate privacy enhancement facilities. It is necessary, however, for a message's originator to be cognizant of whether a message's intended recipient implements privacy enhancements, in order that encoding and possible encryption will not be performed on a message whose destination is not equipped to perform corresponding inverse transformations. (Section 4.6.1.1.3 of this RFC describes a PEM message type, "MIC-CLEAR," that represents a signed, unencrypted PEM message in a form readable without PEM processing capabilities yet validatable by PEM-equipped recipients.) The defined mechanisms are compatible with a range of mail transport facilities within the Internet.